

**REMARKS**

Claims 1, 3, 4, 6-12, 16-29 and 31-33 are pending. By this Amendment, claims 1, 12 and 31 are amended and claims 5 and 30 are cancelled without prejudice or disclaimer. Reconsideration in view of the above amendments and following remarks is respectfully requested.

**I. CLAIMS 1, 3, 4, 6-12, 16-29 AND 31-33 DEFINE PATENTABLE SUBJECT MATTER PURSUANT TO 35 U.S.C. §103**

The Office Action rejects claims 1, 3-12, and 16-29 and 31-33 under 35 U.S.C. §103 as being anticipated by U.S. Patent No. 6,971,028 to Lyle et al. ("Lyle") in view of U.S. Patent No. 6,769,066 to Botros ("Botros"). The rejection is respectfully traversed.

The Office Action asserts that

[i]t would have been obvious to one of ordinary skill in the art at the time of the invention to include human behavior of Botros with Lyle, the motivation is that most attempted security violations are internal; that is, they are attempted by employees of an enterprise or organization (see col.1, lines 48-52). Botros discloses detecting computer network intrusions is calculated based upon factors such as command sequences, user activity, machine usage loads, resource violations, files accessed, data transferred terminal activity and network activity. These factors or [sic] input to a model or expert system which determines whether a possible violation has occurred (see col. 1, lines 53-63). Thus, this is a [sic] method detects misuse of users within a network. It would have been obvious to one of ordinary skill in the art at the time of the invention to include identifying presence of at least one activity and assigning a binary representation to the activity of Botros et al. with Lyle, the motivation is that by identifying and assessing a

binary rating using a histogram of Botros shows the feature values of all users over a predetermined period of time (see col., 11, lines 35-38).

Lyle is directed to a system for tracking the source of computer attacks and the system disclosed in Lyle relies upon receiving data that is associated with an attack and then associating that data with an event. According to Lyle, the data may be received from another administrative domain external to the network concerning the attack or potential attack that is being tracked by another administrative domain. Such data may be received: 1) as an e-mail message received by a network security administrator providing information concerning an attack or suspected attack being experienced by another administrative domain; or 2) from another administrative domain without human intervention in the form of a message received by a tracking system via its network connection containing information concerning the attack or the suspected attack.

In Lyle, a “sniffer” module continuously scans for data being received at various ports of various network devices. The sniffers search for data indicating an actual or suspected attack. The data is queued so that known signature attacks can be analyzed by a tracking system. Post-attack analyses are then shared within the network.

Botros discloses a system and apparatus for training a neural network using historical data from users as well as an artificial set of features reflecting anomalous behavior. In Botros, a normal is created and then a deviation from the normal is observed. Thus, Botros provides for anomaly detection after a network has been characterized. Botros requires samples of current activity on a specific network to differentiate between intrusive behavior and regular network activity.

In contrast, the Applicant’s invention provides a system and method whereby behaviors are rated based upon the presence of expertise and deception and a neural network is trained to return a rating for expertise and deception for any combination of human behaviors that are observed. According to the Applicant’s invention, all of the neural network expertise and deception engines are developed prior to their deployment on any network. Thus, the pre-trained

neural network receives behavior information received from a network and a behavioral assessment is made for each IP/user.

The Applicant's invention provides a back propagation network (BPN) that provides a combined expertise and deception (E/D) rating for each single monitored behavior, as well as for specific combinations of monitored behaviors. The BPN in accordance with the invention is capable of providing the E/D combined rating for any possible combination of behaviors monitored. This feature of the present invention provides for E/D assessments that far exceed the relatively small number of examples used for training. This is in contrast with prior art rule-based signature detection systems whereby every determination made must be stated as a defined rule.

The Applicant's invention can be contrasted with signature detection systems that are restricted by making a one to one correspondence between detections and a threat/no threat decision. The Applicant's invention, in contrast, is capable of presenting the level of expertise and deception present for any given monitored behavior with all possible combinations of all other monitored behaviors. Unlike Applicant's invention, a signature detection system cannot detect a new event if there is no predefined rule for that event.

Thus, the combination of Lyle and Botros fail to provide the Applicant's invention as recited in claim 1. Specifically, Lyle and Botros fail to teach or suggest collecting continuous and sequential samples of port specific information from the received packet level activity information for each IP/user wherein many packets are accumulated in any one sampling interval for each IP/user, as recited in claim 1. Lyle and Botros also fail to teach or suggest recognizing predefined and specific human behavior elements associated with normal and malicious activity from the accumulated packets in a sample of packet level activity and indicating the presence of absence of these predefined behaviors and activities for each IP/user with a designation of 1 (=present) or 0 (=absent), as recited in claim 1.

Furthermore, Lyle and Botros fail to teach or suggest processing in real-time the presence or absence of identified behavior elements for each IP/user occurring within a set sampling interval with a pre-trained neural network behavior assessment pattern classifier into behavior

assessment measures of the amount of “expertise” and “deception” present for each IP/user for a given sampling interval as measures of underlying malicious or non-malicious intent, the trained pattern classifier converting any combination of the predefined behavior elements present for an IP/user for any sampling interval to non-signature and non-anomaly based, pattern classifier determined, assessments of the level of expertise and deception represented by the behavior elements present for that IP/user’s sampling interval, as recited in claim 1.

Therefore, Applicant respectfully requests withdrawal of the rejection of claim 1 under 35 U.S.C. §103. Furthermore, it is respectfully submitted that dependant claims 3, 4, 6-11, 32 and 33 are likewise allowable for the reasons described above and for the additional features which those claims recite.

With respect to independent claim 12, Lyle and Botros also fail to disclose a back propagation network that provides combined expertise and deception ratings for each single monitored behavior, as recited in claim 12. Therefore, Applicant respectfully requests withdrawal of the rejection of claim 12 under 35 U.S.C. §103. Furthermore, it is respectfully submitted that dependant claims 16-29 are likewise allowable for the reasons described above and for the additional features which those claims recite.

With respect to independent claim 31, Lyle and Botros also fail to disclose computer readable program code configured to cause the computer to process in real-time the presence or absence of identified behavior elements for each IP/user occurring within a set sampling interval with a pre-trained neural network behavior assessment pattern classifier into behavior assessment measures of the amount of “expertise” and “deception” present for each IP/user for a given sampling interval as measures of underlying malicious or non-malicious intent, the trained pattern classifier converting any combination of the predefined behavior elements present for an IP/user for any sampling interval to non-signature and non-anomaly based, pattern classifier determined, assessments of the level of expertise and deception represented by the behavior elements present for that IP/User’s sampling interval, and wherein if operator determined thresholds for degree of expertise and deception are exceeded, a network connection blocking action is activated automatically, as recited in claim 31. Therefore, Applicant respectfully

requests withdrawal of the rejection of claim 31 under 35 U.S.C. §103.

Therefore, Applicant respectfully submits that the subject matter of Claims 1, 3, 4 6-12, 16-29 and 31-33 would not have been obvious to one of ordinary skill in the art at the time of Applicant's invention, are therefore not unpatentable under 35 U.S.C. §103. Therefore, withdrawal of the rejection of claims 1, 3-12, 16-29 and 31-33 under 35 U.S.C. §103 is respectfully requested.

## Conclusion

In view of the foregoing, Applicant respectfully requests reconsideration and the allowance of the above-identified application. Should the Examiner feel that there are any issues outstanding after consideration of this response, the Examiner is invited to contact Applicant's representative at the telephone number listed below.

If there are any other fees due in connection with the filing of this response, please charge the fees to our deposit account at Deposit Account No. 50-2821. If a fee is required for an extension of time under 35 U.S.C. 1.136 not accounted for above, such an extension fee is requested and the fee should be also be charged to our Deposit Account.

Respectfully submitted,

Cermak Kenealy & Vaidya LLP



By: \_\_\_\_\_/avaidya/

Ajit J. Vaidya

Registration No. 43,214

## U.S.P.T.O. Customer Number 39083

Cermak Kenealy & Vaidya LLP  
515 E. Braddock Rd., Suite B  
Alexandria, Virginia 22314

703.778.3584 (v)

703.652.5101 (f)

Date: September 21, 2007